## Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

*Please submit responses to dig-comments@nist.gov by March 24, 2023*

***Organization:*** *Nok Nok Labs, Inc*

***Name of Submitter/POC:*** *Rolf Lindemann*

***Email Address of Submitter/POC:*** [REMOVED]

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | NIST SP 80063A | 5.4 | 31 | 1190 | Pairing of IAL3 with AAL2 and AAL2+FAL2 is not intuitive. | Add reasoning to clarify why that pairing makes sense |
| 2 | NIST SP 80063A | 5.5.8 | 31 | 1209 | Supervised Remote ID Proofing is last section: mDL, eID and VCs are upcoming technologies that in general could be suitable for unsupersied remote ID Proofing. It would be great to show where they fit and what the minimum requirements (on a high level) are to achieve IAL3. | Add section 5.5.9 "Requirements for IAL3 Unsupervised Remote Identity Proofing" where mobile Drivers License (mDL), electronic ID cards, Verifiable Credentials etc. are handled |
| | | | | | | |
| 3 | NIST SP 80063B | 5.1.3.1 | 21 | 863 | Clarify requiremenmts for key storage regarding key exportability: It sounds like an underlying Single-Factor/MF Cryptographic *Device* is assumed here - as opposed to SF/MF Crypto SW which allows the exportability of keys. | Clarify whether key exportability is allowed here or not |
| 4 | NIST SP 80063B | 5.1.8.1 | 21 | 1157 | Key export is allowed, but use of exported keys not covered explicitly: Background are multidevice passkeys (FIDO). The traditional single-device (or device-bound) FIDO credentials in some way are managed by a "self-contained" authenticator. Meaning the security only depends on the discrete authenticator. In the case of multi-device credentials (MDCs), the security depends on the discrete authenticator *and* the security of the "Sync-Fabric" plus its communication with Authenticators. That is similar to the trust model of SIM cards which can be linked to phone numbers by the issuing mobile network operator (remember all the SIM Swap issues).<br>Note: an alternative approach could be to always require authenticator being self-contained. Meaning that the discrete HW SecurityKey (ordevice with platform authenticator) *plus* the sync-fabric together would be defined as the "Authenticator".<br>Also: correct typo: "requirementss" | (a) Add statement that exported keys are still subject to requirement in line 1151. (b) Additionally, add statement that means that ability to restore (make usable) such exported key to additional devices requires IAL2/AAL2/FAL2 level protection. (c) And clarify what happens if restoring such (exported) key to new devices is governed by IAL1 or IAL0 identity proofing (in the case no appropriate authenticator is available). |
| 5 | NIST SP 80063B | 5.1.9.1 | 30 | 1186 | Confusing term in this context "Removed": It is not relevant in this context whether the key still is available on "this device", but whether it is available outside as well. | Replace "(i.e., cannot be removed)" with "(i.e., cannot be extracted)" |
| 6 | NIST SP 80063B | 5.1.9.1 | 30 | 1202 | "an authenticator be either a separate piece of HW or an embedded processor…" - the user verification should be seen as part of the authenticator as well: Background: Need to clarify that even (single-device keys in) platform authenticators can be a MF Cryptographic Device - not only Security Keys. | Clarify that the authenticator often includes the user verification component as well - not only the crypto chip/engine. Additionally, clarify that FIDO authenticators supporting single-device credentials (either "legacy" FIDO credentials or device public keys (DPK) typically could meet that requirement). |
| 7 | NIST SP 80063B | 5.2.4 | 34 | 1340 | Attestation is a good way to support requirement in line 1573 in Authenticator Binding. | Explicitly mention that attestation is a strong way for the RP to verify the "type of user-provided" authenticator. Suggest to add a clarifying statement about the consequences of NOT being able to verify the "type of user-provided" authenticator. |
| 8 | NIST SP 80063B | 6.1 | 41 | 1573 | Attestation is a good way to support requirement in line 1573 in Authenticator Binding: This especially applies to authenticators that allow the key export so the RP could verify that exported keys are handled appropriately - see also comment #4 regarding line 1157 above. | Mention that attestation as define in section X provides a strong way for the RP to verify the "type of user-provided" authenticator. |
| 9 | NIST SP 80063B | 8.1 | 52 | 1940 | Authenticator duplication threat | Mention Multi-factor cryptographic SW since key export is allowed here as well.<br>Clarify the applicability to authenticators implementing "multi-device passkeys" and the related Sync-Fabric. |
| 10 | NIST SP 80063B | 8.2 | 55 | 1944 | Mitigation strategies for Authenticator duplication | Mention sync-fabrics/"passkey providers" implementing stringent AAL2/IAL2/FAL2 for restoring multi-device keys that have been backed up as one potential strategy. |
| | | | | | | |
| 12 | NIST SP 80063C | 6.1.2.2 | 39 | 1360 | RP Managed Bound Authenticator needs clarification: Mentioning the TOFU concept really helped me understanding the "Bound Authenticator" approach | Mention trust-on-first-use (TOFU) concept for the "Bound Authenticator". |